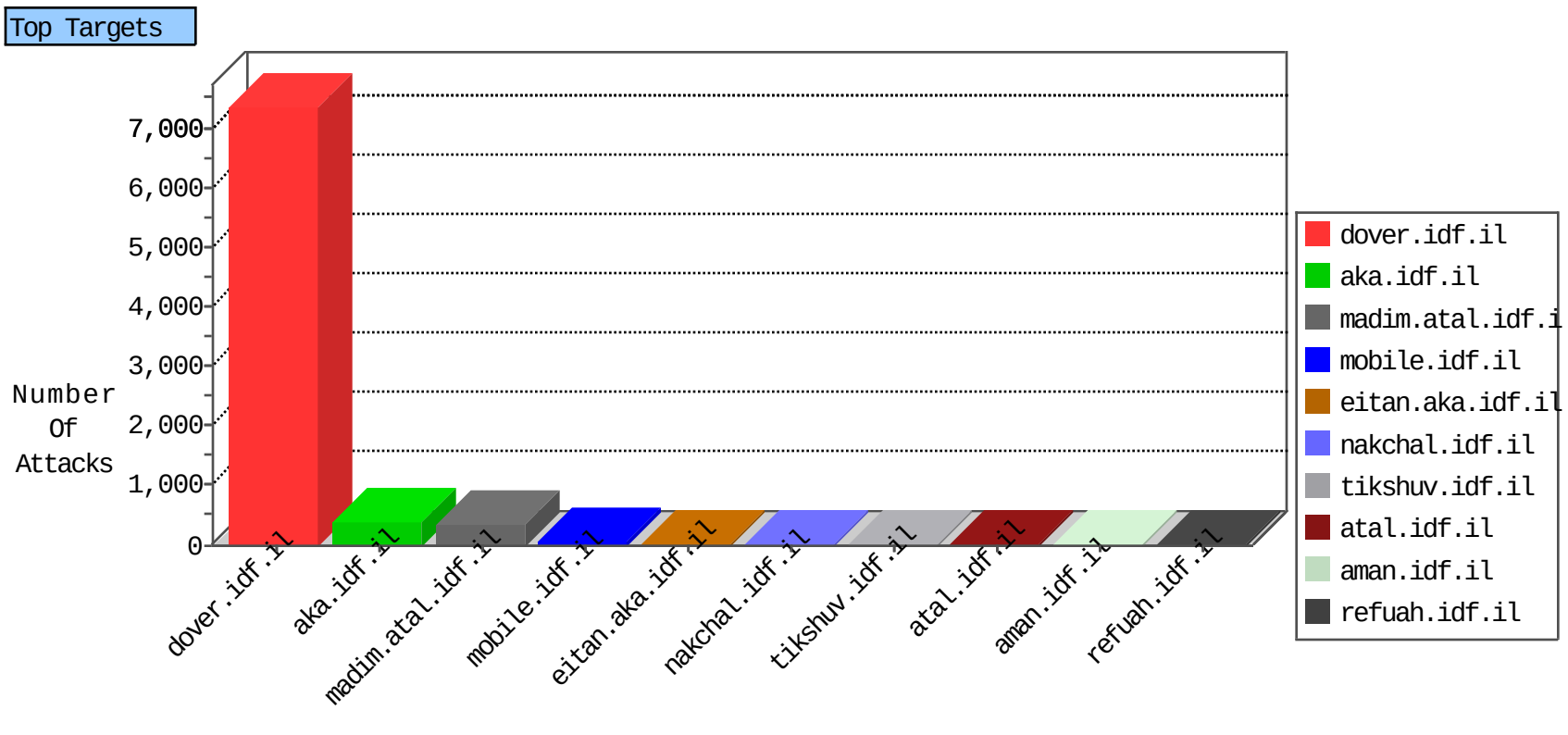
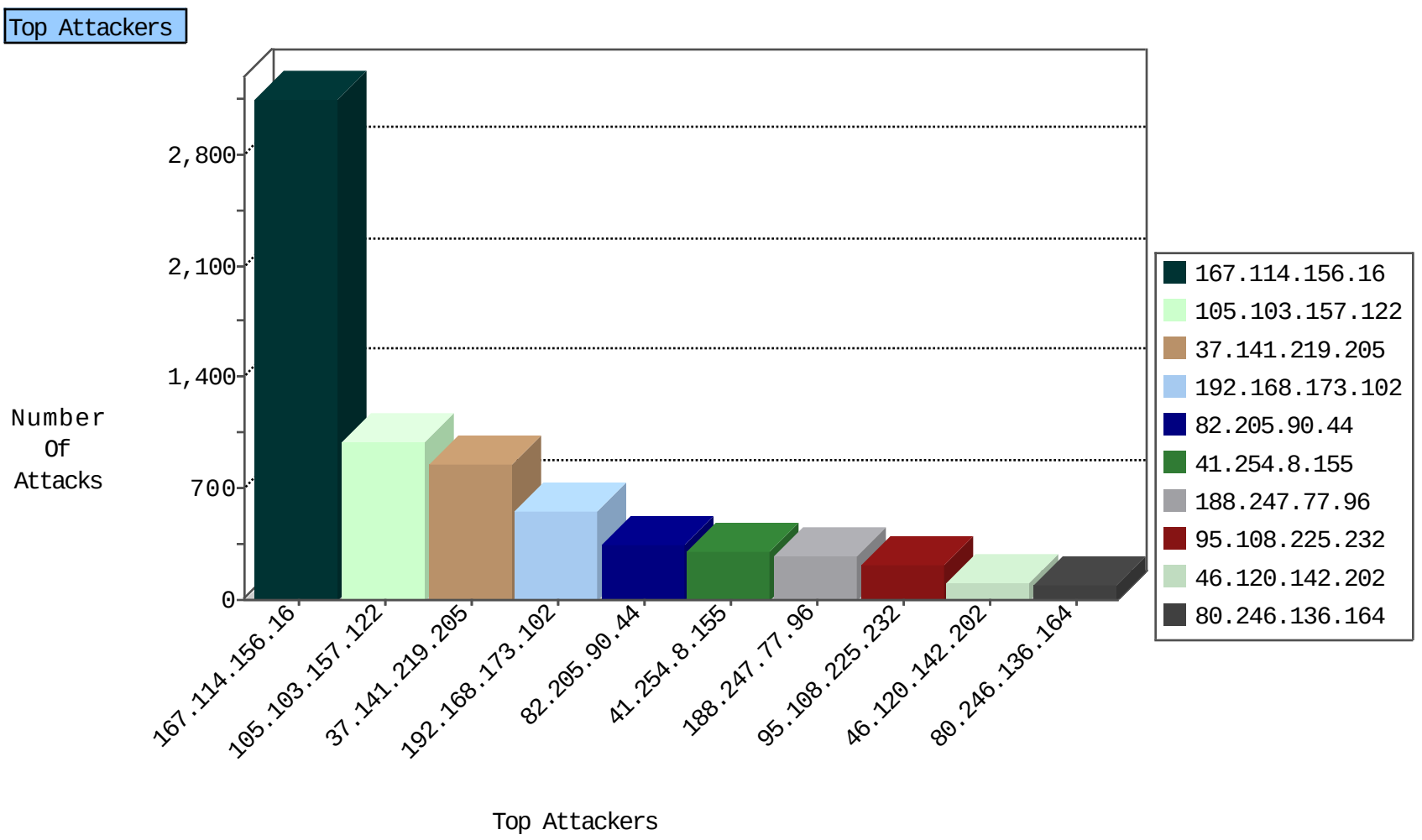
04-07-2016-17:04:01 to 04-07-2016-18:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-07-2016-17:04:01 to 04-07-2016-18:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	3132
105.103.157.122	Algeria	147.237.77.216	dover.idf.il	HTTP-MISC-DoS-GoodBye-30	dest-reset	1544
82.205.90.44	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	341
41.254.8.155	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	307
188.247.77.96	Jordan	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	54
37.8.119.61	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	13
114.79.28.169	Indonesia	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	9
37.141.219.205	Saudi Arabia	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5
87.69.201.196	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
168.235.207.154	United States	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
81.218.165.186	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
37.141.219.205	Saudi Arabia	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
212.235.98.139	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
37.8.119.61	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
168.235.207.154	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	2
37.141.219.205	Saudi Arabia	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	2
37.8.119.61	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	1
185.120.125.67	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	1
85.65.54.19	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
37.239.68.12	Iraq	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	1
37.239.68.65	Iraq	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	1
79.177.1.22	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1

04-07-2016-17:04:01 to 04-07-2016-18:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
196.184.62.248	Tunisia	147.237.77.216	dover.idf.il	C1000133: HTTP: Opisrael 2015 - key words and groups	Block	10
84.228.243.103	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
46.19.85.31	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
213.57.205.145	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
213.239.205.207	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
188.50.148.228	Saudi Arabia	147.237.77.216	dover.idf.il	3886: HTTP: Cross Site Scripting in POST Request	Block	1
188.214.249.151	Romania	147.237.77.216	dover.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-07-2016-17:04:01 to 04-07-2016-18:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
192.35.222.17	147.237.77.216	United States	dover.idf.il	ET DOS SSL Bomb DoS Attempt	3
176.13.2.107	147.237.0.19	Israel	madim.atal.idf.il	GPL SCAN myscan	2
176.13.2.107	147.237.0.19	Israel	madim.atal.idf.il	INDICATOR-SCAN myscan	2
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
80.82.78.38	147.237.77.170	Netherlands	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
77.125.135.203	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
188.50.148.228	147.237.77.216	Saudi Arabia	dover.idf.il	GPL WEB_SERVER /etc/passwd	1
46.19.85.211	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
23.102.168.255	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
149.88.186.188	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
146.185.56.118	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.14.151.201	147.237.0.15	Turkey	kosher-kravi.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
108.162.12.43	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
197.115.17.58	147.237.77.216	Algeria	dover.idf.il	portscan: TCP Distributed Portscan	1
87.71.94.43	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
197.2.105.86	147.237.72.14	Tunisia	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
84.108.125.53	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
194.90.39.41	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.177.25.82	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
188.50.148.228	147.237.77.216	Saudi Arabia	dover.idf.il	SQL Injection - Select From	1
46.19.86.186	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
23.102.168.255	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -sS window 4096	1
174.37.194.144	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 4096	1
149.78.54.147	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.8.14	China	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
110.23.57.188	147.237.77.216	Australia	dover.idf.il	portscan: TCP Distributed Portscan	1
199.203.51.201	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
105.103.157.122	147.237.77.216	Algeria	dover.idf.il	portscan: TCP Distributed Portscan	1
197.2.105.86	147.237.72.14	Tunisia	dover.idf.il(old)	ET SCAN Potential VNC Scan 5900-5920	1
85.64.103.199	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

04-07-2016-17:04:01 to 04-07-2016-18:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.141.219.205	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	699
192.168.173.102		147.237.77.216	dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	356
95.108.225.232	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	220
188.247.77.96	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	220
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	206
105.103.157.122	Algeria	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	155
37.141.219.205	Saudi Arabia	147.237.77.216	dover.idf.il	drop		drop	102
105.103.157.122	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	99
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
2.54.151.164	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
37.141.219.205	Saudi Arabia	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	40
121.7.185.71	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
192.118.27.253	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
105.159.121.18	Morocco	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	24
188.161.66.218	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	22
188.161.66.218	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	22
83.244.49.210	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	21
83.244.49.210	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
83.244.49.210	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
80.246.130.208	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
64.246.165.160	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
104.131.147.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
77.235.135.234	Lebanon	147.237.77.216	dover.idf.il	drop	SAM rule	drop	10
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
105.103.157.122	Algeria	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
84.228.16.214	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.197	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
107.167.109.82	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
37.26.149.139	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.179.42.227	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
2.53.33.128	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
168.235.207.154	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
37.141.219.205	Saudi Arabia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
168.235.207.154	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
46.19.85.197	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
109.64.169.198	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
80.178.24.7	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
31.210.186.153	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
185.120.125.67	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	7
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
80.178.24.7	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
83.130.108.165	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.29.57.190	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
132.66.167.110	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.120.142.202	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
80.246.136.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	89
2.52.168.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	53
176.13.2.107	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	49
176.13.16.90	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	23
176.13.4.41	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/milluim/index	Block	21
109.253.150.242	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	10
188.50.148.228	Saudi Arabia	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.50.148.228	Block	6
66.249.84.166	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
176.13.4.41	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/milluim/index	Block	5
109.234.161.36	France	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.234.161.36	Block	4
66.249.84.167	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
212.143.153.7	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	4
185.32.179.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
155.158.41.144	Poland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/dover.aspx/	Block	2
185.120.126.121	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 185.120.126.121	Block	2
109.253.129.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
217.132.61.86	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	2
157.55.39.205	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
2.53.2.177	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
185.120.126.121	Israel	147.237.77.74	law.idf.il	Unauthorized HTTP Method	Block	2
176.13.16.90	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
79.178.151.38	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/6/4466.jpg	Block	2
62.219.99.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.246.136.240	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
188.50.148.228	Saudi Arabia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/4/size220x0/	Block	1
71.227.55.147	United States	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
46.98.160.231	Ukraine	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1398-en/dover.aspx	Block	1
207.46.13.140	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
105.103.157.122	Algeria	147.237.77.216	dover.idf.il	Abnormally Long Request request version	Block	1
80.178.24.7	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
169.229.3.91	United States	147.237.77.235	sviva.idf.il	Illegal Byte Code Character in Header Name	Block	1
8.37.235.186	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
213.151.59.153	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
82.102.169.113	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
188.161.85.168	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.161.85.168	Block	1
71.227.55.147	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
157.55.39.108	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/homepage.aspx	Block	1
46.98.160.231	Ukraine	147.237.77.216	dover.idf.il	Parameter Type Violation lang in www.idf.il/1398-en/dover.aspx	Block	1
212.126.112.38	Iraq	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/arr/	Block	1
105.107.151.192	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/favicon.ico	Block	1
80.178.24.7	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1135-he/atal.aspx	Block	1
169.229.3.91	United States	147.237.77.235	sviva.idf.il	Illegal Byte Code Character in Method ã[[#2]][[#14]]‰p¢:Ó[[#24]][[#24]]¶²[[#28]]ýñv*TÉ-B*.hXý[[#8]]×[[#14]][[#18]][[#21]]¢[[#5]][[#28]][[#18]]Ç0l5¸›«ÐQÀDŽºí—Ð]	Block	1
37.238.240.38	Iraq	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
82.102.169.113	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/milluim/index	Block	1
188.161.85.168	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar.	Block	1
79.40.196.142	Italy	147.237.77.74	law.idf.il	PHP Attempt	Block	1
105.158.96.153	Morocco	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
80.246.130.208	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter SearchText in www.eitan.aka.idf.il/938-he/eitan.aspx	None	1
68.180.229.241	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-he/cogat.aspx	Block	1